

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-227298

(43)Date of publication of application : 24.08.1999

(51)Int.Cl.

B41J 29/38

G06F 3/12

G06F 13/00

H04L 9/32

(21)Application number : 10-032927

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 16.02.1998

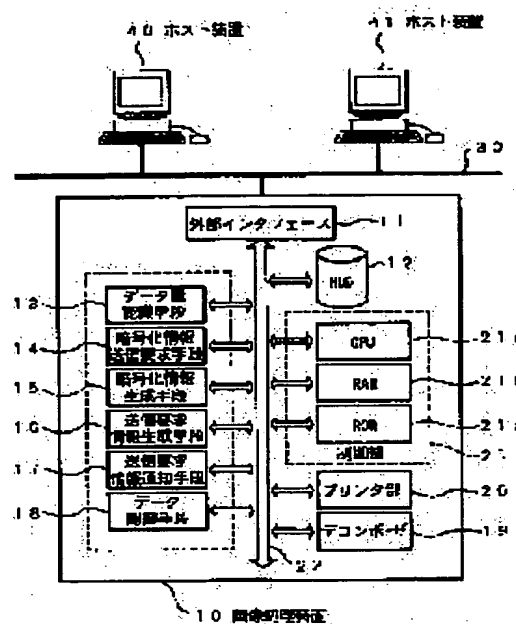
(72)Inventor : EGUCHI HIROYUKI

(54) IMAGE PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To output a data quickly without causing any lowering of throughput due to encryption of data even when a high volume data or a high priority data is outputted.

SOLUTION: This image processor 10 for decrypting a encrypted data from host units 40, 41,... and outputting a visible image comprises means 13 for receiving a data to be outputted after making a decision whether the data satisfies specified conditions or not, and means 14 for requesting the host units 40, 41,... transmitting the data to encrypt the data only when the specified conditions are satisfied.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-227298

(43) 公開日 平成11年(1999) 8月24日

(51) Int.Cl. ⁸	識別記号	F I	
B 4 1 J 29/38		B 4 1 J 29/38	Z
G 0 6 F 3/12		G 0 6 F 3/12	A
			C
	13/00		3 5 1 Z
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A
審査請求 未請求 請求項の数4 O L (全 10 頁)			

(21) 出願番号 特願平10-32927

(22) 出願日 平成10年(1998) 2月16日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 江口 博行

神奈川県海老名市本郷2274番地 富士ゼロ

ックス株式会社海老名事業所内

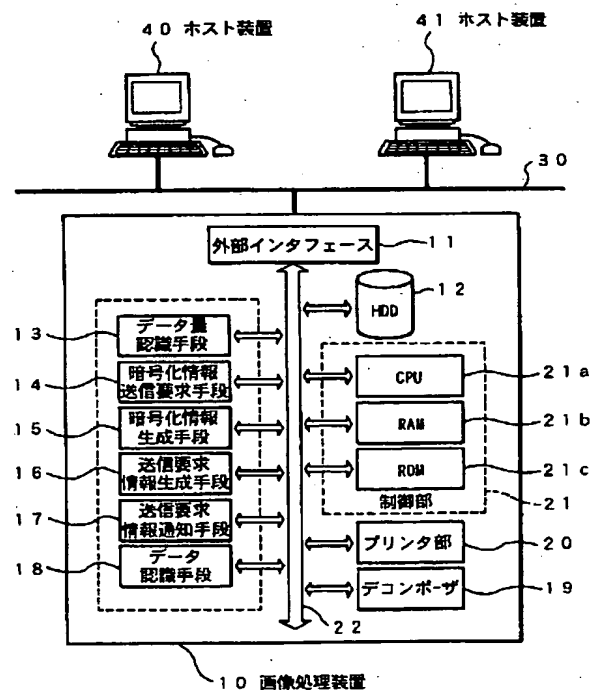
(74) 代理人 弁理士 船橋 國則

(54) 【発明の名称】 画像処理装置

(57) 【要約】

【課題】 データ量の多いデータや出力優先度の高いデータを出力する場合であっても、データの暗号化によるスループットの低下を招くことがなく、迅速なデータ出力を可能とする。

【解決手段】 上位装置40、41…からのデータが暗号化されている場合にはこれを解読した後に可視画像として出力する画像処理装置10において、出力すべきデータを受け取るのに先立ちそのデータが所定条件に該当するか否かを判断する判断手段13と、所定条件に該当する場合にのみ前記出力すべきデータの送信元の上位装置40、41…にそのデータに対する暗号化を要求する要求手段14とを備える。



【特許請求の範囲】

【請求項 1】 上位装置に接続され、該上位装置から送信されるデータを受け取ると該データを可視画像として出力するとともに、前記上位装置からのデータが暗号化されている場合にはこれを解読した後に出力を行う画像処理装置において、

出力すべきデータを受け取るのに先立ち、該データが所定条件に該当するか否かを判断する判断手段と、前記判断手段が所定条件に該当すると判断した場合にのみ、前記出力すべきデータの送信元の上位装置に該データに対する暗号化を要求する要求手段とを備えることを特徴とする画像処理装置。

【請求項 2】 前記判断手段は、前記出力すべきデータのデータ量を認識し、その認識結果が所定量以下である場合に該データが所定条件に該当すると判断するものであることを特徴とする請求項 1 記載の画像処理装置。

【請求項 3】 前記判断手段は、前記出力すべきデータの出力優先度を認識し、その認識結果が所定値より低い場合に該データが所定条件に該当すると判断するものであることを特徴とする請求項 1 記載の画像処理装置。

【請求項 4】 前記出力すべきデータの送信元の上位装置に該データに対する暗号化を要求するか否かを選択するための選択設定手段が設けられたことを特徴とする請求項 1、2 または 3 記載の画像処理装置。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、例えばネットワークプリンタのように、ネットワーク上において用いられ、受信したデータを可視画像として出力する画像処理装置に係わり、特にセキュリティ確保のために暗号化されたデータについても対応可能である画像処理装置に関するものである。

【0002】

【従来の技術】 近年、インターネットと呼ばれる広域ネットワークシステム等の急激な広がりにより、ネットワーク内におけるデータ通信が頻繁に行われるようになっている。これに伴い、ネットワーク内で通信されるデータへの不正アクセスの防止や、データの発信元と送信先との間の認証等のために、データのセキュリティに関する様々な技術が提案されている。

【0003】 例えば特開平 6-44122 号公報には、ネットワーク内で通信されるデータを暗号化することにより、不正アクセスや不正利用の防止を徹底したものが開示されている。これによると、ネットワーク内で画像出力を行う画像処理装置は、ホストコンピュータやプリンタサーバ等の上位装置から送信されるデータを出力するに際し、上位装置との間で暗号化情報の授受を行うようになっている。詳しくは、画像処理装置では、データの送信元となる上位装置に対してそのデータのセキュリティ機能の使用許可を問い合わせた後に、上位装置か

ら暗号化キーが付加されたデータを暗号化情報として受信する。そして、受信した暗号化情報を解読するための演算を行って出力すべきデータを得た後に、その出力すべきデータを可視画像として出力する。

【0004】

【発明が解決しようとする課題】 しかしながら、上述した従来の画像処理装置では、上位装置が所定単位のデータ毎、例えば画像処理装置へ送信するメディア（文字、図形、音声、静止画、動画像など）毎に、暗号化キーを付加してこれを暗号化情報とするため、データを出力するのにあたって、暗号化情報を解読するための演算を頻繁に行うこととなる。したがって、例えば、データ量の多いデータ（ページ数の多い文書等）を出力する場合には、暗号化情報を解読するための演算に多くの時間を必要とし、結果として迅速なデータ出力を行うことができなくなってしまう。また、例えば、ネットワーク内でデータの出力優先度を設定可能となっている場合に、出力優先度の高いデータ（緊急を要する文書等）であっても、暗号化情報を解読するための演算によって、これを出力するまでに多くの時間を費やしてしまう可能性がある。

【0005】 つまり、上述した従来の画像処理装置では、出力すべきデータのすべてに暗号化が行われるので、例えばデータ量の多いデータや出力優先度の高いデータを出力する場合に、暗号化解読のために多くの時間を要してしまい、結果として装置としてのスループットが低下してしまうこととなる。

【0006】 そこで、本発明は、例えばデータ量の多いデータや出力優先度の高いデータを出力する場合であっても、データの暗号化によるスループットの低下を招いてしまうことがなく、迅速なデータ出力を行うことのできる画像処理装置を提供することを目的とする。

【0007】

【課題を解決するための手段】 本発明は、上記目的を達成するために案出された画像処理装置で、上位装置に接続され、その上位装置から送信されるデータを受け取るとこのデータを可視画像として出力するとともに、前記上位装置からのデータが暗号化されている場合にはこれを解読した後に出力を行う画像処理装置において、出力すべきデータを受け取るのに先立ち、そのデータが所定条件に該当するか否かを判断する判断手段と、前記判断手段が所定条件に該当すると判断した場合にのみ、前記出力すべきデータの送信元の上位装置にそのデータに対する暗号化を要求する要求手段とを備えることを特徴とするものである。

【0008】 上記構成の画像処理装置によれば、出力すべきデータを受け取るのに先立ち、判断手段が、そのデータが所定条件に該当するか否かを判断する。ここで、例えばそのデータのデータ量が所定量以下であったり出力優先度が所定値より低い場合のように、そのデータが

所定条件に該当すると判断手段が判断すれば、要求手段は、出力すべきデータの送信元の上位装置にそのデータに対する暗号化を要求する。つまり、出力すべきデータが所定条件に該当していなければ、そのデータに対する暗号化を要求しない。したがって、この画像処理装置では、例えばデータ量が所定量より多いデータや出力優先度が所定値より高いデータのように、所定条件に該当しないデータを出力する場合に、そのデータに対する暗号化を解読する必要がなくなる。

【0009】

【発明の実施の形態】以下、図面に基づき本発明に係わる画像処理装置について説明する。

【0010】〔第1の実施の形態〕図1は、本発明に係わる画像処理装置の第1の実施の形態の概略構成を示すブロック図である。図例のように、本実施の形態の画像処理装置10は、LAN（ローカルエリアネットワーク）等のネットワーク30を介して、複数のホスト装置40、41…と接続されているものである。

【0011】ホスト装置40、41…は、それぞれがパーソナルコンピュータやワークステーション等からなるものであり、画像処理装置10で出力すべき印刷データと、この印刷データの属性に関する情報（例えばデータ名、データサイズ、ホスト装置名、ユーザ名等、以下この情報を属性情報と称す）とを、画像処理装置10に対して送信するものである。これら印刷データおよび属性情報は、各ホスト装置40、41…にインストールされているアプリケーションソフトウェア等により作成され、画像処理装置10へ送信される。なお、印刷データとしては、例えばアスキー（ASCII）コード等によって記述されたものがある。

【0012】また、各ホスト装置40、41…は、詳細を後述するように、それぞれが印刷データの暗号化に必要な暗号化キー情報（以下、暗号化キー#1と称す）と、暗号化情報の生成および解読に必要なアルゴリズムを予め備えているものとする。なお、暗号化キー#1は、各ホスト装置40、41…毎に個別のものとなっている。

【0013】このようなホスト装置40、41…に接続される画像処理装置10は、ネットワークプリンタ等からなるものであり、ホスト装置40、41…から送信される印刷データを受け取ると、その印刷データを可視画像として記録用紙上に出力するものである。そのため、画像処理装置10は、外部インタフェース11と、ハードディスク装置（Hard Disk Drive:以下、HDDと称す）12と、データ量認識手段13と、暗号化情報送信要求手段14と、暗号化情報生成手段15と、送信要求情報生成手段16と、送信要求情報通知手段17と、データ認識手段18と、デコンポーザ19と、プリンタ部20と、制御部21と、これらを互いに接続する内部バス22と、を備えている。

【0014】ここで、これらの各部について詳しく説明する。外部インタフェース11は、ネットワークと接続し、このネットワーク30を介してホスト装置40、41…との間の通信を行うためのものである。HDD12は、外部インタフェース11がホスト装置40、41…からの印刷データを受信すると、その印刷データを記憶蓄積するものである。

【0015】データ量認識手段13は、ホスト装置40、41…から送られてくる印刷データのデータ量を、その印刷データに先立って送られてきた属性情報から抽出し、抽出したデータ量と予め制御部21内のメモリ等に設定されている所定量と比較して、印刷データのデータ量が所定量以下であるか否かを判断するものである。なお、所定量は、この画像処理装置10を使用するユーザが任意に変更できるようにしてもよい。

【0016】暗号化情報送信要求手段14は、データ量認識手段13による判断結果に応じて、印刷データの暗号化を許可するか否かのメッセージを、印刷データの送信元のホスト装置40、41…に通知するものである。例えば、暗号化情報送信要求手段14では、データ量認識手段13が印刷データのデータ量が所定量以下と判断すると、送信元のホスト装置40、41…に印刷データの暗号化を許可し、その印刷データに対する暗号化情報の付加を要求する。また、暗号化情報送信要求手段14では、暗号化の要求の応答として、送信元のホスト装置40、41…から暗号化情報を生成するための暗号化キー#1を取得するようになっている。

【0017】暗号化情報生成手段15は、暗号化情報送信要求手段14が取得した暗号化キー#1と、予め制御部21内のメモリ等に保持されている暗号化キー情報（以下、暗号化キー#2と称す）とを基に、所定の暗号化情報生成アルゴリズムに従って演算を行い、その演算によって暗号化情報を生成するものである。なお、暗号化情報およびこれを生成するための暗号化情報生成アルゴリズムは、周知技術を利用したものであるため、ここではその詳細な説明を省略する。

【0018】送信要求情報生成手段16は、HDD12あるいは図示しないバッファメモリの空き容量を基にホスト装置40、41…から受信可能な印刷データのデータサイズを算出し、そのデータサイズに関する情報と暗号化情報とから送信要求情報を生成するものである。送信要求情報通知手段17は、送信要求情報生成手段16が生成した送信要求情報をホスト装置40、41…に送信するものである。

【0019】データ認識手段18は、ホスト装置40、41…から暗号化された印刷データが送られてくると、その印刷データから暗号化情報を抽出し、抽出した暗号化情報に対して所定の暗号化情報照合アルゴリズムに従って演算を行い、その演算結果から暗号化情報が正しいか否かを照合し、送られてきた印刷データに対する認証

を行うものである。なお、暗号化情報照合アルゴリズムも、暗号化情報生成アルゴリズムと同様に、周知技術を利用したものであるため、ここではその詳細な説明を省略する。

【0020】デコンポーザ19は、ホスト装置40、41…から受け取った印刷データに対して、可視画像として出力するために必要な処理を行うものである。例えば、デコンポーザ19では、HDD12から順次取り出したアスキーコード等の印刷データを、プリンタ部20で出力可能なビットマップデータ等の画像データに変換するようになっている。プリンタ部20は、デコンポーザ19が変換した画像データを、周知の電子写真技術を利用して記録用紙上に可視画像として出力するものである。

【0021】制御手段21は、上述した各部、すなわち画像処理装置10全体の動作制御を行うものである。そのために、制御手段21では、CPU (Central ProcessingUnit) 21a、RAM (Random Access Memory) 21bおよびROM (Read Only Memory) 21cを有している。なお、上述した各手段13~18は、この制御手段21での所定プログラムの実行により、機能的に実現されるものである。

【0022】次に、以上のように構成された画像処理装置10において、ホスト装置40、41…からの印刷データを出力する場合の処理動作例について、図2および図3のフローチャートを参照しながら説明する。ただし、ここでは、説明を簡単にするために、ネットワーク30上におけるある1つのホスト装置40から印刷データの出力依頼があった場合を例に挙げて説明する。

【0023】ホスト装置40は、印刷データの出力依頼を行う場合に、まず、印刷データの送信に先立ち、その印刷データについての属性情報を画像処理装置10へ送信する。ホスト装置40が属性情報を送信すると、画像処理装置10では、図2に示すように、外部インタフェース11がその属性情報を受信して（ステップ101、以下ステップをSと略す）、その属性情報を制御部21内のRAM21bに一時的に格納させる（S102）。

【0024】属性情報がRAM21bに格納されると、続いて、画像処理装置10では、データ量認識手段13がその属性情報を基に、ホスト装置40から送られてくる印刷データのデータ量を抽出し（S103）、抽出したデータ量を予め設定されている所定量と比較する（S104）。このとき、抽出したデータ量が所定量より小さければ、暗号化情報送信要求手段14は、印刷データの暗号化を許可する旨のメッセージをホスト装置40に送信し、その印刷データに対する暗号化情報の付加を要求する（S105）。

【0025】一方、ホスト装置40では、印刷データの暗号化を許可する旨のメッセージを受け取ると、そのメッセージに応じて、このホスト装置40が予め備えてい

る暗号化キー#1を、画像処理装置10に対して送信する。

【0026】ここで、ホスト装置40からの暗号化キー#1を外部インタフェース11が受信すると（S106）、暗号化情報生成手段15は、その暗号化キー#1と、予め画像処理装置10側で保持していた暗号化キー#2とを基に、暗号化生成アルゴリズムに従って暗号化情報（以下、この暗号化情報を第1の暗号化情報と称す）を生成する（S107）。次いで、送信要求情報生成手段16は、その時点において受信可能な印刷データのサイズを算出して、これをホスト装置40に送信を要求する印刷データのサイズとする（S108）。そして、送信要求情報生成手段16は、その印刷データのサイズに関する情報と先に暗号化情報生成手段15が生成した第1の暗号化情報とから送信要求情報を生成する（S109）。その後、送信要求情報通知手段17は、その送信要求情報をホスト装置40に送信して、その内容をホスト装置40に通知する（S110）。

【0027】送信要求情報をホスト装置40に送信すると、画像処理装置10では、ホスト装置40からの印刷データの受信待ち状態となる（S111）。このとき、ホスト装置40では、送信要求情報を受け取ると、このホスト装置40が備えるアルゴリズムに従って、送信要求情報に含まれる第1の暗号化情報が正しいか否かの照合、すなわち送信要求情報に対する認証を行う。そして、その照合結果が正しいければ、このホスト装置40の暗号化キー#1およびアルゴリズムにより、第1の暗号化情報から新たな暗号化情報（以下、この暗号化情報を第2の暗号化情報と称す）を生成するとともに、画像処理装置10で出力すべき印刷データのうちの送信要求情報で指定されたサイズ分に第2の暗号化情報を付加し、これを画像処理装置10へ送信する。なお、第2の暗号化情報は、第1の暗号化情報と出力すべき印刷データとから生成するようにしてもよい。

【0028】その後、ホスト装置40からの印刷データ（第2の暗号化情報を含む）を外部インタフェース11が受信すると、制御部21は、これらをHDD12内に記憶蓄積する（S112）。そして、データ認識手段18は、HDD12内の印刷データから第2の暗号化情報を抽出するとともに（S113）、暗号化情報照合アルゴリズムに従って、その第2の暗号化情報が正しいか否かの照合、すなわち印刷データに対する認証を行う（S114）。

【0029】このとき、第2の暗号化情報が正しくなければ、制御部21は、HDD12内の印刷データを破棄する（S115）。また、第2の暗号化情報が正しいければ、制御部21は、HDD12内から印刷データを読み出して（S116）、その印刷データをデコンポーザ19に転送する（S117）。そして、デコンポーザ19がその印刷データを画像データに変換するとともに（S

118)、プリンタ部20がその画像データを記録用紙上に出力する(S119)。制御部21は、HDD12内の印刷データの全てについて終了するまで、これらのステップ(S116~S120)を繰り返す。

【0030】これらのステップ(S116~S120)が終了すると、次に、制御部21は、先にデータ量認識手段13が認識した印刷データのデータ量の全てについて、ホスト装置40からの受信が終了しているか否かを判断し(S121)、終了していなければ、再び未受信の印刷データを受信するステップ(S111)から上述したステップを繰り返し、データ量の全てについて終了するまでこれを続行する(S111~S121)。

【0031】また、データ量認識手段13による判断の結果(S104)、抽出したデータ量が所定量よりも大きければ、図3に示すように、暗号化情報送信要求手段14によるメッセージの送信や暗号化情報生成手段15による第1の暗号化情報の生成を行わずに、送信要求情報生成手段16が算出した受信可能な印刷データサイズを(S122)、そのままの状態(第1の暗号化情報を付加せずに)ホスト装置40へ送信する(S123)。ここで、画像処理装置10では、ホスト装置40からの印刷データの受信待ち状態となる(S124)。

【0032】その後、ホスト装置40からの印刷データを外部インタフェース11が受信すると、制御部21は、これをHDD12内に記憶蓄積する(S125)。ただし、このとき、ホスト装置40からは、指定したサイズの印刷データのみが送信され、第2の暗号化情報については送信されない。これは、暗号化情報送信要求手段14による暗号化情報の付加要求、具体的には送信要求情報生成手段16からホスト装置40への第1の暗号化情報の送信が行われていないからである。

【0033】そして、制御部21は、HDD12内から印刷データを読み出して(S126)、デコンポーザ19による画像データへの変換を経て(S127、S128)、プリンタ部20での出力を行わせる(S129)。制御部21は、これをHDD12内の印刷データの全てについて終了するまで繰り返し(S124~S130)、さらにはホスト装置40から受信すべき印刷データの全てについて終了するまで上述したステップを繰り返す(S124~S131)。

【0034】以上のように、本実施の形態の画像処理装置10では、出力すべき印刷データのデータ量が所定量以下である場合にのみ、その印刷データの送信元のホスト装置40、41…に暗号化を要求するようになっている。すなわち、出力すべき印刷データのデータ量が所定量よりも多ければ、その印刷データに対する暗号化情報の付加を要求しないので、その印刷データの出力に際し、暗号化情報の照合、すなわち暗号化の解読を行う必要がない。

【0035】したがって、この画像処理装置10を用い

れば、データ量の多い印刷データ(ページ数の多い文書等)を出力する場合には、暗号化解読のための演算を頻繁に行う必要がなくなり、そのために多くの時間を費やしてしまうこともないので、従来よりも迅速な印刷データの出力を行うことができるようになる。これは、特に、ホスト装置40、41…との間で所定単位の印刷データ毎、例えば画像処理装置へ送信するメディア(文字、図形、音声、静止画、動画像など)毎に、暗号化を行うように構成されている場合に有効である。

【0036】つまり、この画像処理装置10では、出力すべき印刷データのデータ量が所定量よりも多い場合であっても、印刷データの暗号化によるスループットの低下を防ぐことが可能となるので、従来よりも迅速な印刷データの出力を実現することができるようになる。

【0037】なお、本実施の形態では、画像処理装置10がホスト装置40、41…からの印刷データを出力する場合を例に挙げて説明したが、本発明はこれに限定されるものではない。例えば、図4に示すように、LAN30上にサーバ装置50が設けられているシステムについても、本発明は適用可能である。この場合、ホスト装置40、41…からの印刷データは、サーバ装置50により識別番号が割り当てられた後に、サーバ装置50内のプリントキューに蓄えられ、画像処理装置10での出力が可能であるとサーバ装置50が判断すると、プリントキュー内から順次画像処理装置10へ送信される。よって、このようなシステムにおいても、画像処理装置10がサーバ装置50からの印刷データのデータ量に応じて、そのデータ量が所定量以下である場合にのみ、サーバ装置50における暗号化キー#1(パブリックキー)と画像処理装置10における暗号化キー#2(プライベートキー)とに基づく暗号化を行うようにすれば、上述した場合と同様の効果を得ることができる。

【0038】また、本実施の形態では、印刷データのデータ量に応じて暗号化を要求するか否かを判断する場合を例に挙げて説明したが、本発明はこれに限定されるものではない。例えば、ホスト装置40、41…において印刷データの出力の緊急度を表す出力優先度が設定されるとともに、その出力優先度に応じて画像処理装置10(またはサーバ装置50)が印刷データの処理順序を決定するように構成された場合に、画像処理装置10は、属性情報から出力優先度に関する情報を抽出して、これが所定値より低いかなかを判断し、所定値より低ければ暗号化を要求するようになることも考えられる。このようにすれば、出力優先度の高い印刷データ、すなわち緊急を要する印刷データについては、暗号化解読の演算のために多くの時間を費やしてしまうことがなくなるので、迅速な出力が可能となる。つまり、ユーザの所望する出力(緊急出力等)を実現できるので、ユーザにとっては便利なものとなる。

【0039】〔第2の実施の形態〕次に、本発明に係わ

る画像処理装置の第2の実施の形態について説明する。ただし、ここでは、上述した第1の実施の形態と同一の構成要素については、同一の符号を与えてその説明を省略し、第1の実施の形態の場合との相違点についてのみ説明する。

【0040】図5は、本発明に係わる画像処理装置の第2の実施の形態の概略構成を示すブロック図である。図例のように、本実施の形態の画像処理装置10aは、第1の実施の形態で説明したものに加えて、液晶タッチパネル23と、暗号化情報付加手段24と、が設けられているものである。

【0041】液晶タッチパネル23は、画像処理装置10aを使用するユーザが操作するためのもので、この画像処理装置10aにおけるコンフィグレーション情報の設定やその変更を行うためのものである。この操作手段2-3で行う設定の一例としては、ホスト装置40、41…からの印刷データについて暗号化を要求するか否かを選択するための設定がある。

【0042】暗号化情報付加手段24は、制御手段21での所定プログラムの実行により、機能的に実現されるものであり、液晶タッチパネル23での設定結果に応じて、印刷データに対する暗号化を要求するか否かを選択するものである。ただし、暗号化情報付加手段24では、不揮発性のメモリであるNVRAM (nonvolatile Random Access Memory) を有しており、このNVRAM内に暗号化を要求するか否かを判断するための暗号化フラグを保持するようになっている。つまり、暗号化情報付加手段24では、液晶タッチパネル23での設定結果に応じて変更される暗号化フラグに基づいて、ホスト装置40、41…が印刷データを送信する際のセキュリティ機能として暗号化情報を付加するか否かを選択するようになっている。

【0043】ここで、液晶タッチパネル23での暗号化を要求するか否かの設定について、図6および図7を参照しながら説明する。図5は、暗号化を要求するか否かを設定する際の液晶タッチパネル23における表示内容の具体例を示す説明図であり、図6は、暗号化を要求するか否かを設定する際の手順を示すフローチャートである。

【0044】この画像処理装置10aでは、図6(a)に示すように、ユーザにより液晶タッチパネル23上の「メニュー」(アイコン)が押下されると(図7におけるS201)、液晶タッチパネル23がメニュー一覧を表示する(図7におけるS202)。このとき、ユーザにより「メンテナンス」が選択されると(図7におけるS203)、液晶タッチパネル23は、図6(b)に示すように、メンテナンスする項目を表示する(図7におけるS204)。次いで、ユーザによりメンテナンスする項目のうちの「オプションセッティ」が選択されると(図7におけるS205)、液晶タッチパネル23は、

図6(c)に示すように、オプション一覧を表示する(図7におけるS206)。その後、ユーザによりオプション一覧のうちの「アンゴウカ」が選択されると(図7におけるS207)、液晶タッチパネル23は、図6(d)に示すように、ユーザに「オン」か「オフ」を選択させる。ここで「オン」が選択され(図7におけるS208)、その後「スタート」(アイコン)が押下されると(図7におけるS209)、液晶タッチパネル23は、「オン」が選択された旨を暗号化情報付加手段24に通知する。そして、暗号化情報付加手段24は、液晶タッチパネル23からの通知に従って、NVRAM内の暗号化フラグを、「オン」が選択された旨に対応する「1」(TRUE)に書き換える。このようにして、暗号化を要求するか否かの設定が行われる。

【0045】次に、以上のような画像処理装置10aにおいて、ホスト装置40、41…からの印刷データを出力する場合の処理動作例について、図8および図9のフローチャートを参照しながら説明する。ただし、ここでも、ある1つのホスト装置40から印刷データの出力依頼があった場合を例に挙げて説明する。

【0046】この画像処理装置10aでは、上述したように、液晶タッチパネル23で暗号化を要求するか否かの設定が行われると、図8に示すように、暗号化情報付加手段24がNVRAM内の暗号化フラグを書き換えて変更することにより、その設定内容を保持しておく(S301)。なお、この暗号化フラグは、次の印刷データを処理するときから反映され、画像処理装置10aの電源がオフされても保持される。

【0047】ここで、ホスト装置40から属性情報の送信があると、この画像処理装置10aでは、第1の実施の形態の場合と同様に、外部インタフェース11がその属性情報を受信し、RAM21bに一時的に格納させる(S302~S303)。

【0048】ただし、この画像処理装置10aでは、ホスト装置40からの属性情報がRAM21bに格納されると、第1の実施の形態の場合とは異なり、暗号化情報付加手段24が暗号化フラグのチェックを行う。詳しくは、暗号化情報付加手段24は、NVRAM内の暗号化フラグが「1」(TRUE)であるか否かを判断する(S304)。

【0049】そして、暗号化フラグが「1」(TRUE)であれば、この画像処理装置10aでは、暗号化情報送信要求手段14が印刷データの暗号化を許可する旨のメッセージをホスト装置40に送信し(S305)、以下、第1の実施の形態の場合(図2におけるS106~S121参照)と同様の処理を行う(S306~S321)。また、暗号化フラグが「1」(TRUE)でなければ、この画像処理装置10aでは、図9に示すように、暗号化情報送信要求手段14によるメッセージの送信を行わずに、以下、第1の実施の形態の場合(図3におけ

る S 1 2 2 ~ S 1 3 1 参照)と同様の処理を行う (S 3 2 2 ~ S 3 3 1)。

【0050】 以上のように、本実施の形態の画像処理装置 1 0 a では、液晶タッチパネル 2 3 での暗号化を要求するか否かの設定に応じて、暗号化情報付加手段 2 4 が暗号化フラグを変更するとともに、この暗号化フラグに基づいて暗号化情報送信要求手段 1 4 が印刷データの暗号化を要求するようになっている。すなわち、暗号化を要求するか否かを、液晶タッチパネル 2 3 から選択し得るようになっている。したがって、この画像処理装置 1 0 a を用いれば、ユーザは、スループットの低下を防いで迅速な出力を実現するか、あるいは印刷データのセキュリティを確保するか、を任意に選択できる。これにより、この画像処理装置 1 0 a は、ユーザにとっては非常に便利なものになるとともに、システムとしての汎用性を高めることも可能となる。

【0051】 なお、本実施の形態では、液晶タッチパネル 2 3 での設定結果のみに応じて、印刷データに対する暗号化を要求するか否かを選択する場合を例に挙げて説明したが、本発明はこれに限定されるものではなく、第 1 の実施の形態で説明した場合との組み合わせを実現してもよい。この場合には、例えば、暗号化情報送信要求手段 1 4 が、印刷データのデータ量が所定量以下であり、かつ、暗号化フラグが「1」(TRUE)である場合に、印刷データの暗号化を許可する旨のメッセージをホスト装置 4 0、4 1 … に送信することが考えられる。

【0052】

【発明の効果】 以上に説明したように、本発明の画像処理装置は、出力すべき印刷データが所定条件に該当する場合にのみ、その印刷データの送信元の上位装置に暗号化を要求するようになっている。すなわち、印刷データが所定条件に該当しなければ、その印刷データに対する暗号化を要求しない。したがって、所定条件に該当しない印刷データについては、その出力に際し暗号化の解読を行う必要がないので、そのために多くの時間を費やしてしまうことがなく、従来よりも迅速な出力を実現し、

スループットが低下してしまうことを防ぐことができる。

【図面の簡単な説明】

【図 1】 本発明に係わる画像処理装置の第 1 の実施の形態の概略構成を示すブロック図である。

【図 2】 第 1 の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート(その 1)である。

【図 3】 第 1 の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート(その 2)である。

【図 4】 第 1 の実施の形態の画像処理装置の応用例を示すブロック図である。

【図 5】 本発明に係わる画像処理装置の第 2 の実施の形態の概略構成を示すブロック図である。

【図 6】 暗号化を要求するか否かを設定する際の液晶タッチパネルにおける表示内容の具体例を示す説明図であり、(a)はメニュー一覧の具体例の図、(b)はメンテナンスする項目の具体例の図、(c)はオプション一覧の具体例の図、(d)は暗号化を要求するか否かの設定画面の具体例の図である。

【図 7】 暗号化を要求するか否かを設定する際の手順を示すフローチャートである。

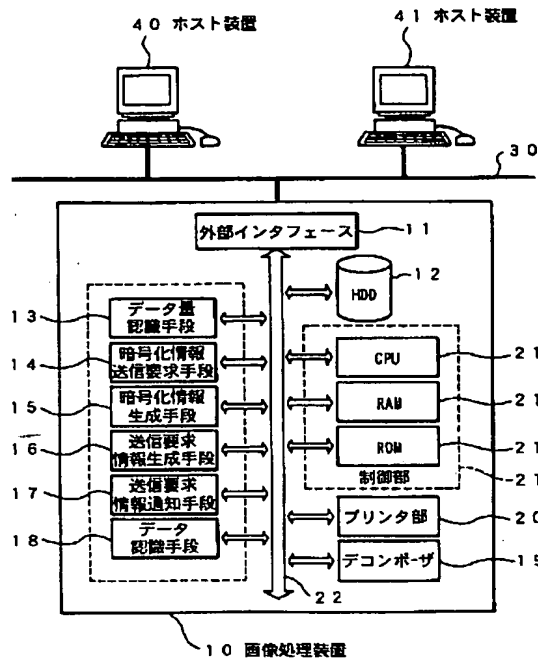
【図 8】 第 2 の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート(その 1)である。

【図 9】 第 2 の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート(その 2)である。

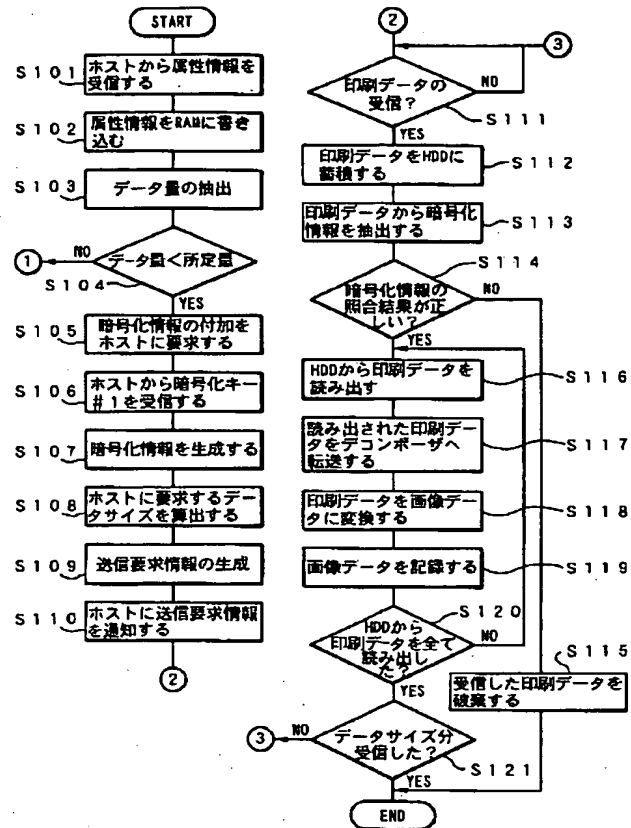
【符号の説明】

1 0 … 画像処理装置、1 3 … データ量認識手段、1 4 … 暗号化情報送信要求手段、1 5 … 暗号化情報生成手段、1 6 … 送信要求情報生成手段、1 7 … 送信要求情報通知手段、1 8 … データ認識手段、2 3 … 液晶タッチパネル、2 4 … 暗号化情報付加手段、4 0、4 1 … ホスト装置、5 0 … サーバ装置

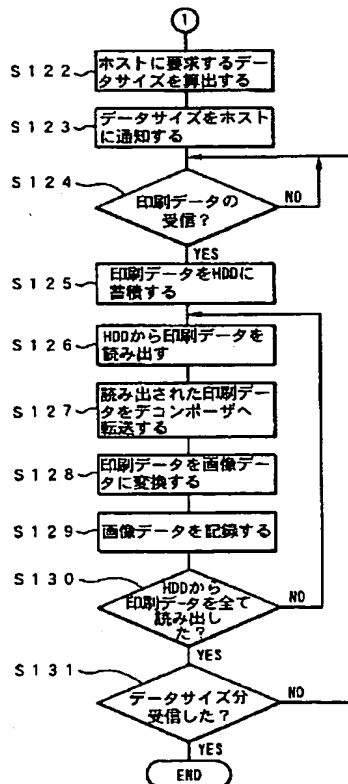
【図1】



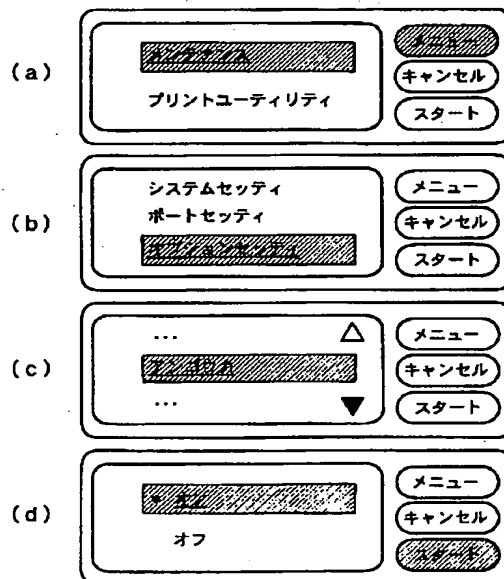
【図2】



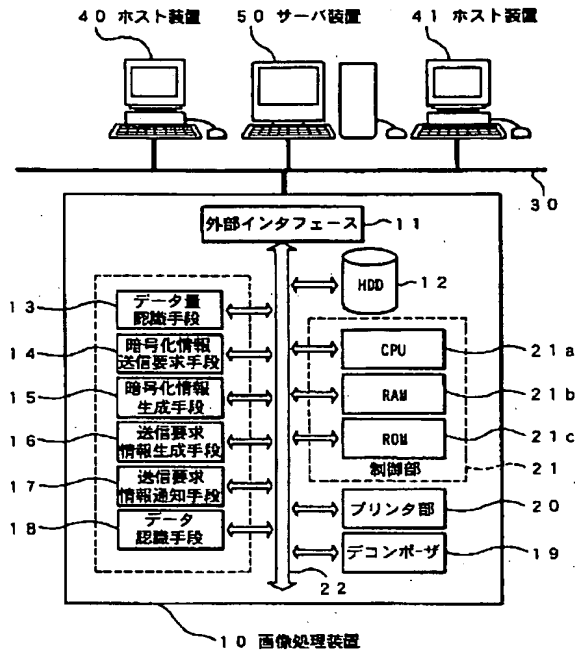
【図3】



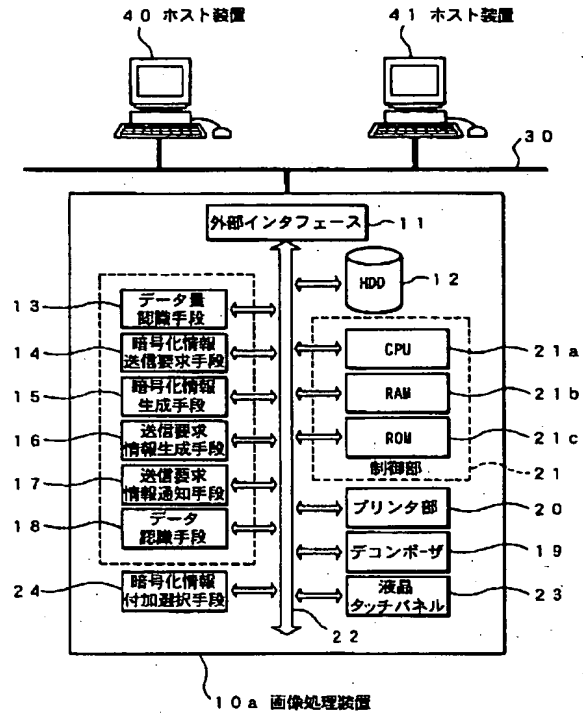
【図6】



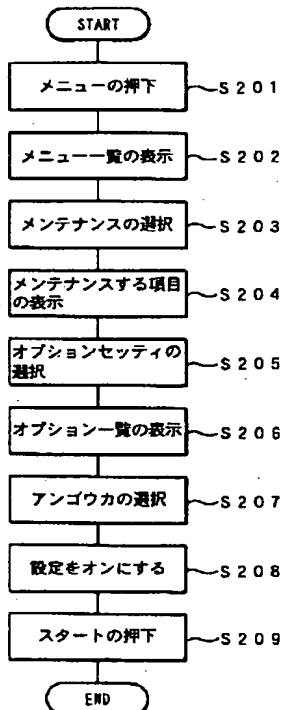
【図 4】



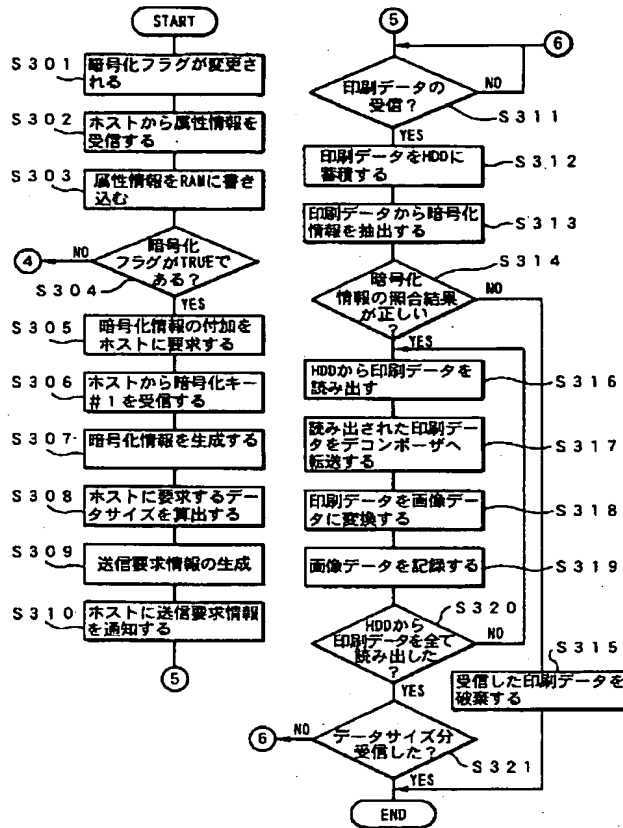
【図 5】



【図 7】



【図8】



【図9】

